bitcoin

BITCOIN:
Moneda y Mercados

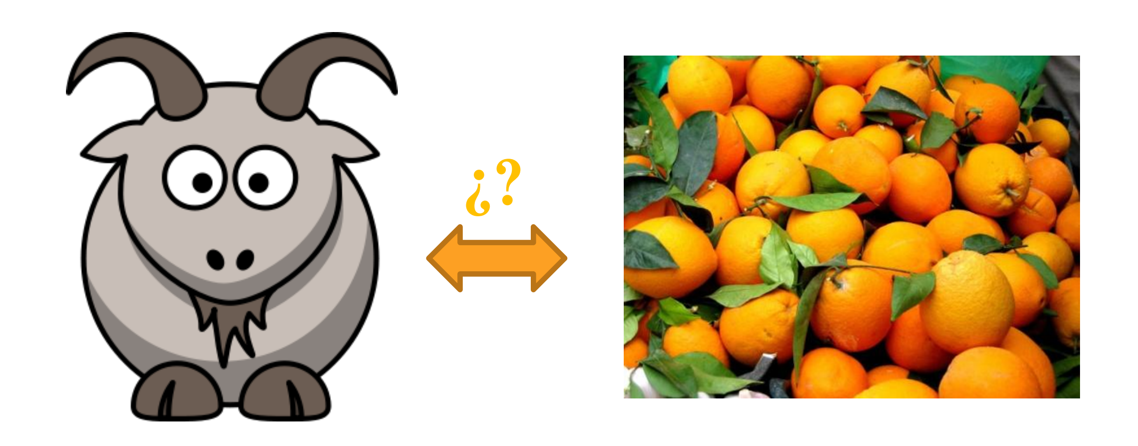
ÍNDICE

- Historia
- Características
- Cómo se manejan
- Evolución
- Mercados



Historia – El Dinero

- Inicialmente, se hacía trueque.
  - "Te cambio mi cabra por esas naranjas"



  - ¿Y si no las quiero todas ahora porque se estropean?
  - ¿Y si no quiero tantas naranjas? ¿Cómo fracciono la cabra?
  - ¿Y si no quiero naranjas realmente?



Historia – El Dinero

- Se empieza a utilizar como trueque otro bien intermedio (sal, metales, etc.)

- Aparece el oro como metal de intercambio
  - No se estropea
  - Es fácilmente divisible
  - Se puede recomponer
  - Fácil de contar/cuantificar al peso
  - Es escaso



- Contravalor real → Contravalor Representativo



Historia – El Dinero

- Finalmente aparece el "dinero fiat"
  - De curso legal por decreto
  - A partir de 1971 sustituye al "patrón oro"
- Los gobiernos pueden imprimir más dinero
  - Inflación
  - Devaluación de la moneda
  - Este tipo de decisiones quedan en manos del gobierno o gobiernos
- Los intercambios monetarios están centralizados



Historia – Bitcoin y criptomonedas

- En 2008 aparece un artículo sobre Bitcoin
  - Satoshi Nakamoto

BTC / XBT

- Se definen:
  - Las bases de la moneda
  - Algoritmos de funcionamiento
  - Tasa de “impresión”
  - Descentralización de las transacciones

- En 2009 aparece la primera implementación de un cliente Bitcoin



Características

- En el cliente, se definen pares de claves pública/privada

- A partir de la clave pública, se obtienen **direcciones**

- Las transacciones se realizan entre direcciones, que no están vinculadas a ninguna persona en concreto
  - Las transacciones son públicas
  - Los *exchanges* o mercados pueden exigir identificación



Características: Pero… ¿qué es un bitcoin?

- Un bitcoin es un **apunte contable**, que indica que en una dirección, hay una cantidad de dinero.
- Estos apuntes se inscriben en **bloques**
  - Se almacenan **transacciones**
  - Un valor que "resuelve" el bloque
  - El *hash* del bloque anterior
- De este modo, los bloques quedan enlazados, formando una cadena de bloques: **Blockchain**
  - Esta cadena contiene todas las transacciones
  - El tamaño del *blockchain* actual es de 15 GB



Características: ¿Cómo se generan?

- Se trata de un reto criptográfico.

- Es preciso encontrar la cadena (*nonce*) que haga que el doble *hash* SHA256 del bloque empiece por un número definido de ceros
  - En el bloque se introduce una transacción adicional, desde el *coinbase* a una dirección definida por el usuario

- Se trata de probar combinaciones de forma aleatoria hasta dar con la solución
  - Se hace una analogía con la búsqueda de oro: **mineros**



Características:
¿Cómo se generan?

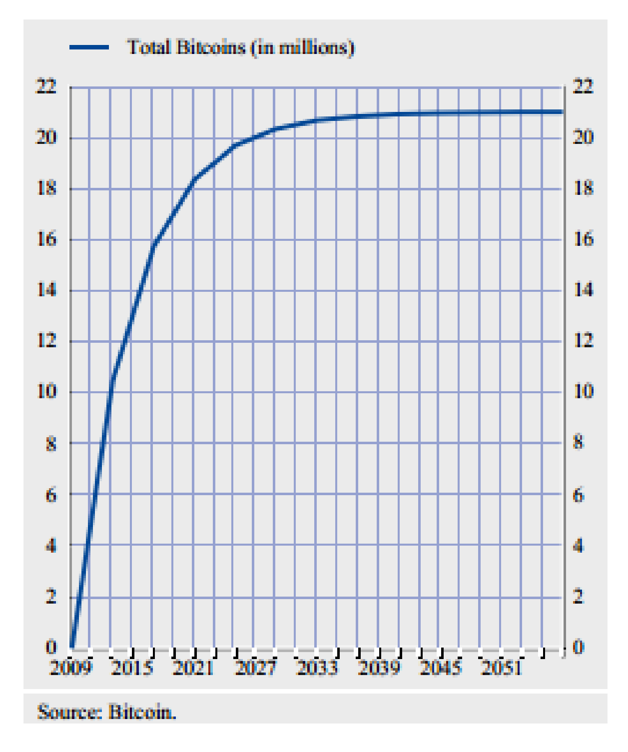


Características:
¿Cómo se generan?



CARACTERÍSTICAS: ¿CÓMO SE GENERAN?

- La tasa de generación de bitcoins está fijada en el algoritmo



- Según aumenta la potencia de cálculo de la red se aumenta la complejidad – 1 bloque / 10 minutos



Características: ¿Cómo se generan?

Hash Rate
Source: blockchain.info

Hash Rate GH/s

40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0

Apr '13 May '13 Jun '13 Jul '13 Aug '13 Sep '13 Oct '13 Nov '13 Dec '13 Jan '14 Feb '14 Mar '14

Difficulty
Source: blockchain.info

Difficulty

5,000,000,000
4,000,000,000
3,000,000,000
2,000,000,000
1,000,000,000
0

Apr '13 May '13 Jun '13 Jul '13 Aug '13 Sep '13 Oct '13 Nov '13 Dec '13 Jan '14 Feb '14 Mar '14



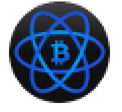
¿Cómo se manejan?

- Existen varios tipos de clientes (y *wallets*)

- *Offline* completos
  - Necesitan sincronizar la cadena de bloques entera
    - Cliente oficial: bitcoin-qt 
    - Armory 
    - 15 GB de datos

- *Offline* con sincronización externa
  - Utilizan servidores externos
    - Electrum Multibit
    - Hive Bitcoin wallet







¿Cómo se manejan?

- Carteras *online*
  - Blockchain.info
  - Coinbase
  - Coinkite

- La cartera o *wallet* contiene las claves criptográficas asociadas a los bitcoins.

- Si la cartera se pierde (se borra del disco duro, se olvida al contraseña de acceso), los bitcoins se pierden.



Manejo - Riesgos

- Si un sitio *online* sufre un ataque y las claves privadas son robadas, todos los bitcoin de los usuarios se roban.
  - Es el equivalente a un robo en un banco, pero sin que haya garantía de devolución (al menos de momento)

- Se han desarrollado *troyanos* tanto para ordenadores como para móviles que buscan robar los ficheros de los *wallet* de las víctimas.
  - Se recomienda siempre proteger estos ficheros con contraseña.



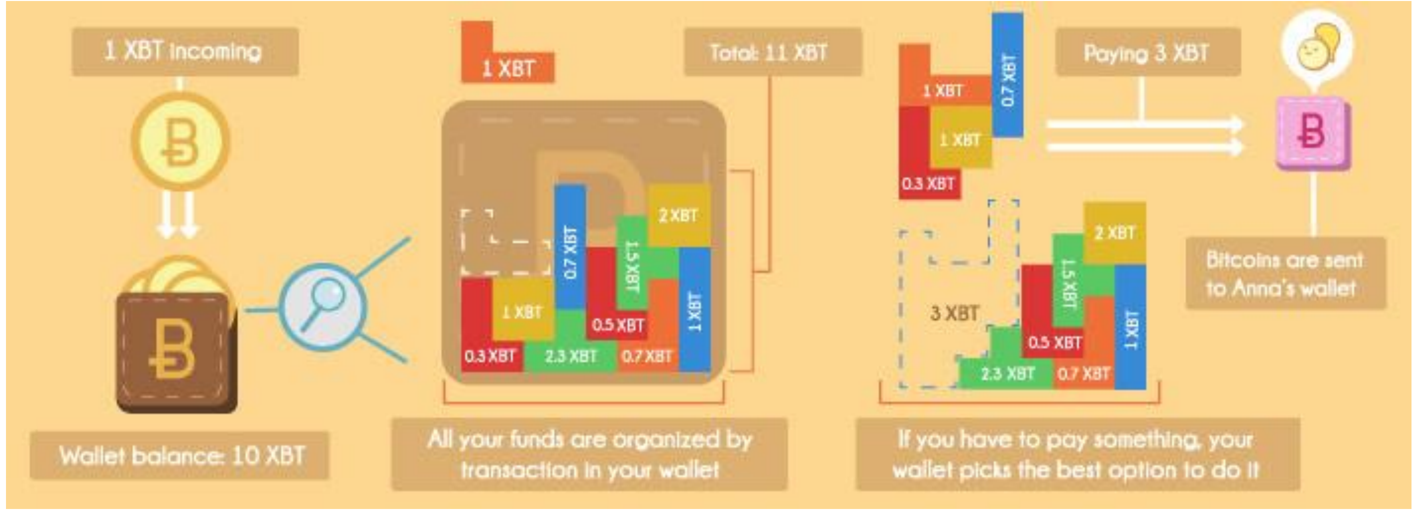
Transacciones

- Las transacciones se publican a la red:
  - Se envían BTCs desde una dirección a otra
- Cada 10 minutos aproximadamente, se añaden al *blockchain*
- Cada vez que se realiza una transacción, ésta puede llevar una pequeña comisión
- El *minero* que añada las transacciones al bloque recibe esa comisión.



TRANSACCIONES









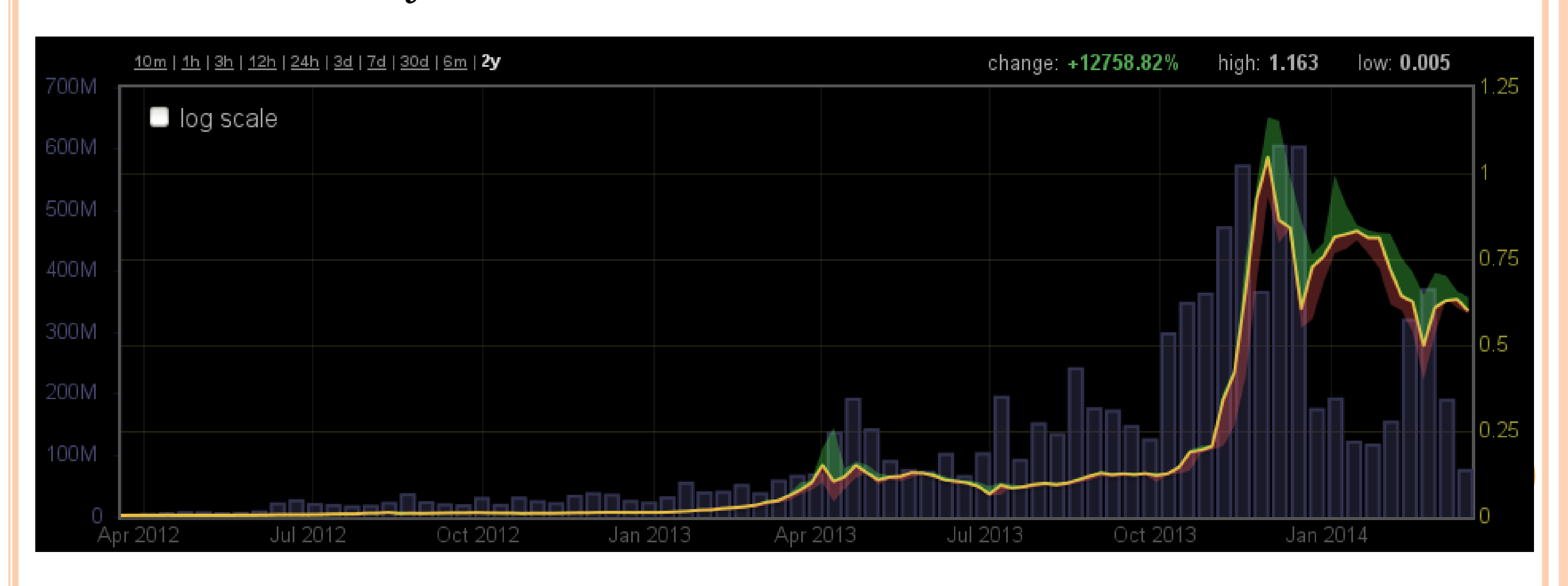
Transacciones

- Si más de un *minero* genera una solución, pueden existir varias versiones del *blockchain*.
- La cadena más larga es la que prevalece.
- La recompensa actual por añadir un bloque es de 25 XBT
  - En 2017 se reducirá a 12,5 XBT
- Además de la comisión de las transsacciones



Evolución

- En 2009, prácticamente no había volumen y el precio era de unos pocos céntimos
- A partir de 2012 se ve un aumento en la cotización y movimientos



EVOLUCIÓN

- El uso de bitcoin no está plenamente regulado
- Hay incertidumbre al respecto
  - Los precios tienen una gran volatilidad
- En países como Alemania, su uso está exento de impuestos (pero sólo se permite el pago entre particulares)
- En China se ha prohibido que las instituciones financieras lo utilicen
- Estas noticias afectan a la cotización:
  - https://www.tradingview.com/e/wB3NBBLp/



Evolución: eventos

Bitcoin / Dollar, D, MTGOX O 13.50 H 13.63 L 13.45 C 13.53
Vol (20) 6.104K 27.093K

REALTIME

BTCUSD, Bitcoin / Dollar

gold parity; 1 bitcoin = 1 troy ounce of gold

China issued regulation notice that Bitcoin is not a currency, and banned financial and payment institutions from starting Bitcoin related business, while allowing exchanges and people to freely use Bitcoin in accordance

Bitfinex glitch causes all sorts of craziness for a few hours; all trades in the period reversed shortly therafter; in other news, Apple pulls Blockchain.info app from the App Store causing outrage among the Bitcoin users

MtGox blames Bitcoin transaction malleability for withdrawal delays; Bitcoin core developers and Bitcoin Foundaton refute the claims. In the end it turns out that the Mt. Gox's custom wallet implementation failed to upgrade to a change in Bitcoin protocol from a year ago which was done specifically to alleviate malleability issues.

The UK's tax agency has reversed an earlier ruling that classified virtual currencies as gift vouchers, exempting digital currency trading from a 20% value added tax (VAT)

On February 28th 20... files for bankruptcy ... with an outstanding ... $63.6m, finally admi... 850k bitcoins were l...

Crash influenced ... of bitcoin, forgets a...

Bitcoin-24 shuts down as its bank account in Poland is confiscated under allegations that they received money from stolen accounts in Deutsche Bank

Paul Krugman criticises Bitcoin from a Keynesian standpoint;

MtGox bankruptcy

first official Bitcoin conference in San Jose

First customer receives ASIC miner from Avalon.

-823.77 (-90.02%)

A major vulnerability in the Bitcoin protocol was spotted. Transactions weren't properly verified before they included in the blockchain which let users bypass Bitcoin's economic restrictions and create an indefinite number of bitcoins.

Bitcoin Savings and Trust shuts down, becoming largest Bitcoin heist in the history, with 263024 bitcoins lost

1300.00, 1200.00, 1100.00, 1000.00, 900.00, 800.00, 700.00, 600.00, 500.00, 400.00, 300.00, 200.00, 135.00, 100.00, 0.00, 48.306K

Aug, 2011, 29, 2012, Jun, 2013, Jun, 2014, Jun, 2015



MERCADOS

- Existen numerosos mercados o *exchanges*

- Se intercambia dinero *fiat* por BTCs

- Existen varios modelos:
  - Cuenta online de dinero y bitcoins
    - Mt.Gox, Bitstamp, Kraken

  - Intermediarios (garantes)
    - Bitcoin-de, Localbitcoins



MERCADOS

- El 45% de los *Exchanges* han fracasado [1]
- Los *exchanges* más grandes sufren numerosos ataques
- El tiempo medio de vida es de 381 días
  - El 30% de los *exchanges* cierran durante el primer año
- Mt.Gox, uno de los grandes, ha quebrado en 2014



[1] http://www.wired.co.uk/news/archive/2013-04/26/large-bitcoin-exchanges-attacks

Mercados: Mt Gox

Market Price (USD)
Source: blockchain.info

Market Price (USD)

1,400
1,200
1,000
800
600
400
200
0

Apr '13 May '13 Jun '13 Jul '13 Aug '13 Sep '13 Oct '13 Nov '13 Dec '13 Jan '14 Feb '14 Mar '14

- No se sabe qué va a pasar
- De momento el dinero y los BTCs están bloqueados



Historias

- Alrededor de los bitcoin han surgido numerosas historias y anécdotas.
- El mercado negro “Silk Road” utilizaba como medio de pago bitcoins.
- Surgió en 2011 y fue clausurada por el FBI en 2013
- Se confiscaron 614.305 bitcoins
  - Al cambio del momento, unos 28,5 millones de $



Historias

- "La pizza"
  - En 2010 una persona logró que la pizzería en la que hacía los pedidos aceptase 10.000 BTCs por 2 pizzas
  - En 2013 el BTC llegó a cotizar a $1.200, de modo que esos 10.000 BTCs llegaron a poder ser vendidos por $12 millones (ahora sería más o menos la mitad)

- "El apartamento de Oslo"
  - Kristoffer Koch, noruego, gastó unos $27 en 2009 comprando 5000 bitcoins, y se olvidó de ellos.
  - En 2013 los vendió obteniendo alrededor de $850.000
  - Con parte de los beneficios se compró un piso en una de las zonas más cotizadas de Oslo, al contado.



HISTORIAS

- "El disco duro"
  - En el Reino Unido, alguien que también había adquirido los bitcoin cuando su cotización era muy baja, tiró a la basura el disco duro donde los tenía almacenados.
  - Se estima que el valor de los bitcoins almacenados oscilaba entre los 7,5 y 9 millones de dólares en 2013



BIBLIOGRAFÍA

- Wikipedia
- http://bitcoin.it
- http://bitcoinfees.com
- Bitcoin: curso seguridad (Universidad Rey Juan Carlos, URJC)
- https://blockchain.info
- https://bitconity.org



Dudas o preguntas

Jonás Andradas Arias

@jandradas

http://www.linkedin.com/in/andradas

¿Dónde usar los bitcoins?

- Existen numerosos sitios online que aceptan bitcoins
- Sitios de juego *online*
- Servicios *online* (VPNs, servidores virtuales, etc.)
- Billetes de avión: CheapAir.com
- Especias online: Spicescave.com



¿Dónde usar los bitcoins?

- Se pueden buscar negocios y tiendas en:
  - http://coinmap.org/
  - http://www.bitcoinmaps.org/
  - http://www.aceptamosbitcoin.com/
  - http://usebitcoins.info

